

LEVERAGE

INFORMATION SYSTEMS

WHITE PAPER

PRESENTED BY :



EMISSION SECURITY

**Reducing the emissions of Information Technology
reduces the risk of information loss**

James D. Heimberg, ABC, Ph.D., ISSO

April 6, 2007

Overview

Across a darkened street, a windowless van is parked. Inside, an antenna is pointed out through a fiberglass panel. The antenna is aimed at an office window on the third floor. As the physician works on a Microsoft Word document that represents some of the notes for a patient record and that describe the complex medical condition of the Chief Executive Officer (CEO) of a Fortune 500 company, the doctor never suspects that what appears on his monitor is being captured, displayed, and recorded in the van below.

During 1997, such an occurrence did happen at a major university medical center. The result was that the stock of the company was devalued based on the health issues of the CEO, and the company ultimately declared bankruptcy.

The ability to read the electronic emissions of Information Technology (IT) equipment is a severe problem for any organization that deals with sensitive or classified information on its IT equipment. As a result, the Federal government implemented a program, which is referred to as Emission Security (EMSEC), to deal with the emissions. Another term sometimes used synonymously is TEMPEST. TEMPEST may be an acronym for Transient ElectroMagnetic Pulse Emanation STandard; however, that has never been documented as such and the term also may have been derived from the storm (tempest) that was created by discovery of this specific emissions vulnerability of electronic equipment.

Today, TEMPEST is a U.S. government description for a set of standards that are intended to limit electric or electromagnetic radiation emissions from equipment such as microchips, monitors, desktop and laptop computers, servers, printers and various peripheral devices.

For EMSEC hardware under Department of Defense control, there are four categories into which such equipment may fall. In order from least restrictive to most restrictive, they are:

- Commercial, Off-the-Shelf (COTS) equipment
- Zone equipment
- TEMPEST equipment
- Zone of Control (ZOC) equipment

Zone, TEMPEST, or ZOC certification must apply to entire systems, not just to individual components, since connecting a single unshielded component (such as a cable) to an otherwise secure system could easily make it radiate dramatically more Radio Frequency (RF) signal. The general principle is that computer monitors and other devices give off electromagnetic radiation. With the right antenna and receiver, these emissions can be intercepted from a remote location, and then be re-displayed.

Equipment with the TEMPEST or EMSEC designation has been tested and the range from which the emissions can be read is much less than that of Zone equipment.

- COTS equipment may be purchased from a variety of vendors with no guarantee with regard to any limitation on the amount of emissions or the range within those emissions can be measured, converted, and read.
- Zone equipment consists of COTS products that are not designed to meet the TEMPEST standards, but have been tested against a portion of that standard and assigned a Zone rating of A through C.
- TEMPEST equipment consist of items specifically remanufactured that meet stringent requirements for the amount of electromagnetic radiation that can be sensed resulting in a distinct range of protection for the equipment in the facility where it is housed.
- ZOC equipment has an even smaller electronic emission signature (range) and is usually TEMPEST equipment that is contained in special shielded enclosures to further reduce emissions.

Certified equipment under the EMSEC program is protected from sale to anyone outside the United States by stringent regulations and each sale must be approved by the Government. This is part of the reason that the equipment is mostly used by Governmental entities at this point. However, there is reason to believe that with laws that control non-Governmental entities (e.g., the Information Technology Management Reform Act [ITMRA], the Health Insurance Portability and Accountability Act of 1996 [HIPAA], Sarbanes-Oxley Act [SARBOX], and the National Infrastructure Protection Program [NIPP]), there may be valid reason for some of the EMSEC equipment to be a desired set of components in the medical, financial, and critical infrastructure industries.

TEMPEST consulting, testing, and manufacturing is a big business in the United States, estimated at over one billion dollars a year. Because of the cost of TEMPEST equipment, the lesser standard called Zone has been implemented. This does not offer the same level of protection as TEMPEST, but it is less expensive, and is used in less-sensitive applications.

TEMPEST or Zone specifications are not designed specifically to equipment. These standards can be applied to an office or an entire building with copper or other conductive materials included in the building materials. Effective protection begins with the physical environment. Unless the wiring can be shielded (telephone lines, electrical wiring, network cables, etc.), all of the security protection to the personal computers and other equipment is not going to stop emissions from leaking to the outside world; emissions can pass from one set of wires to another or even to water pipes.

What are electric or electromagnetic radiation emissions? Unintentional information-bearing signals which, if intercepted and analyzed, disclose private or sensitive information transmitted, received, handled, or otherwise processed by information processing equipment. That is of great concern to industry and is part of the special emphasis of the Federal Network Services, Inc. INFOSEC Services Division.

Emissions Security Methodology

The Federal Communications Commission (FCC) participated in creation of a series of formal standards that are used to evaluate new electronic equipment before that equipment can be offered for public sale. The reason for doing this is that when modern electrical devices operate, they generate electromagnetic fields. This happens with all types of electrical and electronic equipment from computers to radios to microwave ovens to i-Pods. Basically this is true for any equipment with a microchip, diode, or transistor, even with modern refrigerators and other kitchen appliances that are considered smart appliances.

In the case of common, everyday electronics, the new products are taken into a specialized testing laboratory where an engineer completes a complicated battery of tests to ensure that the items will not interfere with other equipment likely to be in the area, whether home or office.

Information Technology (IT) equipment is another consideration due to the data that it uses on behalf of the user and the ability to communicate with other like systems sharing the data. Because of this unique capability of IT equipment to maintain, modify, and transfer data, which creates its usefulness to society, it also is a danger that the information can be read from quite a distance away from the equipment. The emissions from this type of equipment are referred to as "compromising emanations" due to the ability to reconstruct the data remotely and thereby access it without proper credentials that may otherwise be required.

Another way to say it is that compromising emanations are the unintentional intelligence-bearing signals, that, when intercepted and decoded from purely digital formats to the languages used in computers through the processes of analysis and translation, can reveal information that was not intended for those who would use sensitive electronic equipment to receive the emanations.

The next logical step is to realize that if an enterprise deals with information that is sensitive for any reason (e.g., classified, proprietary, personally sensitive, etc.), it has an obligation to protect that information from those who would attempt to obtain it for personal gain. This is the purpose of EMSEC as a function of INFOSEC.

EMSEC technical disciplines typically involve eliminating or reducing the transient compromising emanations caused by a communication signal and the resulting harmonics. The signals and their harmonics can allow the original signal to be reconstructed, analyzed, and translated into useful information.

One of the more common ways to capture and read compromising emanations is to use raster analysis, which is not an overly expensive proposition. A raster analysis capture and translation system can be constructed for well under \$100, which makes capture of valuable information an easy target for those who understand the value of the information being used on the IT systems. Costs for such systems increase with the sensitivity of the equipment.

Determining justification for controlling EMSEC issues is a risk management task that should be conducted at the level of the Chief Information Officer (CIO) of the enterprise. Most enterprises have an Information Assurance (IA) or INFOSEC office in which there is a great deal of knowledge based on the skills of the personnel hired into the roles of Information System Security Officer (ISSO) or a similar

position as well as the Information System Security Engineer (ISSE) or a similar position. Generally speaking, the people who fill those roles have experience based on military service or work within other enterprises where they garnered experience or anecdotal information about EMSEC. The enterprise should rely on these individuals to guide the process.

Process Components

To follow the military model as documented in the *National Security Agency's (NSA's) Zoned Equipment Program (ZEP) Procedures Package*, the process to determine the need for EMSEC should be a three-step process. The steps are:

- Facility Zone Assignment – Facility Zones are determined by measuring the combined attenuation provided by both the free space distance to the control boundary and the physical building structure.
- Equipment Zone Assignment – Equipment Zones are obtained by comparing laboratory test results as specified in National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST/1-92 to specific equipment Zone criteria.
- Matching Zoned Equipment with the Appropriate Facility Zones – Zones are matched to ensure that the radiation from the equipment operating within the facility is reduced to an acceptable level at the nearest control boundary.

This effort should only be undertaken by ISSEs who have TEMPEST certification from the NSA. NSTISSAM TEMPEST/2-95 contains guidance on matching Facility Zones with Equipment Zones. Most of the discriminators are based on the amount of decibels that are measurable in the emissions of electronic equipment; however, with regard to Facility Zones, the equations used translate to distance from the equipment location to the outer boundary of the facility where it is considered that undesirable reading of the emissions will not occur due to the area being what is considered a controlled space. That document states that the inspectable space of the various Zone levels is:

FACILITY ZONE	<i>INSPECTABLE SPACE</i>
A	66 feet
B	>66 up to 328 feet
C	>328 feet

TEMPEST requirements are even more stringent than Zone requirements and ZOC requirements are more stringent than TEMPEST requirements.

Summary

EMSEC is a very controlled technology mostly in use when dealing with foreign national attempts to gain access to critical classified information held by the U.S. Government. Based on established needs, Federal enterprises have access to the applicable equipment needed as approved by NSA.

With changes in the laws regarding the necessity to protect non-Governmental information on IT systems, other organizations are starting to consider how to protect the data and reduce the risk of critical data being provided to unscrupulous personnel who will use it for their own advantage.

In any case, organizations that decide to pursue this level of protection should rely on professionals to determine the exact needs and recommend the right approach. In the past, some have relied on contractors who have taken the organizations' funds and provided no protection or incorrect levels of protection in return. Certain companies have developed the technical capability to determine the right approach and providing the right equipment. The trick is to ensure that the enterprise uses the right approach and gains the needed protection.

The key to a successful IT security program lies in how well systems are documented and evaluated with regard to security issues. Leverage Information Systems' INFOSEC Services Division provides a holistic approach to INFOSEC in general and specifically to C&A efforts for Government and Federally mandated programs to ensure IT systems can be operated safely and securely. In addition, INFOSEC Services provides services that offer Return-On-Investment (ROI) features to increase safe, secure operations of IT systems and to provide for better system protection throughout the life cycle of the system.

For more information, refer to the contact information provided on our Website: www.INFOSEC.leverageis.com and a representative will be happy to provide more information.

Leverage Information Systems is a Value-Added Reseller for some of the most respected providers of EMSEC IT equipment and can provide certified professionals who perform all the implementation and maintenance professional services needed to assist in getting the right equipment needs established, obtaining the equipment that will best suit the enterprise, and keeping that equipment at peak operational performance. In addition, as a Cisco Gold Reseller, we can provide for the best performance of all networking that must be done in support of EMSEC operations.